UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

Civil Case No. 3:14-cv-00491

Dallas Buyers Club, LLC

Plaintiff,

v.

Does 1-20

Defendant

Defendant {John Doe #5, IP address 24.177.125.63} ("Defendant") is identified in Plaintiff's complaint as the Internet Service Provider (ISP) subscriber assigned Internet Protocol ("IP") address 24.177.125.63. As of now, I will be representing myself *Pro Se* in this matter before the Court. I understand that *Pro Se* litigants are required to follow the same rules and procedures as litigants represented by attorneys as seen in *Nielson v. Price,* 17 F.3d 1276, 1277 (10th Cir. 1994). I will abide by these rules and procedures, but ask the courts indulgence as I'm not a lawyer.

I would like to formally oppose the disclosure of the information being requested by the Plaintiff from Charter Communications, Inc. I oppose for the following reasons:

1. Plaintiff's allegations are only based on the fact that Defendant is the Internet Service Provider (ISP) subscriber (pays the ISP bill). Plaintiff alleges Defendant' public IP address was observed for one second on the alleged infringement date. There is NO reasonable information to even suggest that Defendant is the offender; only that the Internet subscription is in his name. No due diligence efforts have been taken to attempt

to identify the true infringer beyond seeking early discovery from the ISP. Plaintiff has voluntarily chosen not to mitigate the alleged damages in its claims.

2. Defendant uses a wireless router to access the internet. A wireless router allows the IP address to be shared with multiple devices, even at the same time. Multiple people have "access" to the router, including but not limited to, a roommate, former neighbors, other various friends and family. Any one of those persons could possibly be the offender, not necessarily the person whose name is associated with the account.

3. Defendant lives in a large apartment building where many people are within range of Defendant's wireless router. This apartment building is located in Madison, WI, near the college campus of University of Wisconsin – Madison. Defendant has seen many young students in his building and feels it is reasonable to assume that most traditional college students today are generally more technologically savvy than the average citizen.

4. Defendant believes it is possible that a number of people could have hacked his wireless router and used his internet and therefore IP address without permission. As mentioned in #3, Defendant lives near many bodies within range of his wireless router. Defendant has taken reasonable steps to secure his wireless router ie: a password is required to access the internet. Despite this fact, Defendant did a quick Google search and found out that with the right software and information, it is not difficult bypass a password. Here is a small excerpt taken directly from this website, http://lifehacker.com/5873407/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver:

> *Your Wi-Fi network is your conveniently wireless gateway to the internet, and since you're not keen on sharing your connection with any old hooligan*

> *who happens to be walking past your home, you secure your network with a password, right? Knowing, as you might, how easy it is to crack a WEP password, you probably secure your network using the more bulletproof WPA security protocol.*
>
> *Here's the bad news: A new, free, open-source tool called Reaver exploits a security hole in wireless routers and can crack most routers' current passwords with relative ease. Here's how to crack a WPA or WPA2 password, step by step, with Reaver—and how to protect your network against Reaver attacks.*
>
> *In the first section of this post, I'll walk through the steps required to crack a WPA password using Reaver. You can follow along with either the video or the text below. After that, I'll explain how Reaver works, and what you can do to protect your network against Reaver attacks.*

Multiple other links have been provided in Appendix 1 if you would like to read more information on how people are able to accomplish this.

5. Defendant never received a notice of the alleged infringement and therefore was not able to inquire for further information or look into any security breaches to prevent future infringements. Since it recorded the first alleged infringement on 16 March 2014, Plaintiff has not sent any Digital Millennium Copyright Act (DMCA) take-down notices to the ISPs. Defendant is an ISP subscriber of Charter Communications, which has DMCA representative on file with the US Copyright Office. The alleged infringement Plaintiff claims are exactly what the DMCA take down notice was designed for. Plaintiff should have sent a DMCA take down notice to Defendants ISP as soon as the offending IP address was noted by its technical monitoring personnel on 16 March 2014. The ISP would have forwarded the DMCA take down notice to ISP subscriber (Defendant) as a normal course of its legal requirement to maintain its "safe harbor" status in accordance with the Online Copyright Infringement Liability Limitation Act. Plaintiff instead chose to allow this alleged infringement activity to persist for over 5 months without taking any

reasonable protective steps to limit the continuing infringement. As Plaintiff waited until Early Discovery was authorized, Defendant and the ISP were not notified of the alleged infringement on Defendants' public IP address until 2 September 2014. Had defendant been notified in a timely manner, he would have taken steps to determine if the activity was happening on his network and to ensure the activity stopped. As Plaintiff claims the unabated copyright infringement of its movies cause significant damage, sending DMCA notices is a reasonable and necessary step (due diligence) to take.

DATED: September 5, 2014

Respectfully submitted,

John Doe #5

Appendix 1

1. http://lifehacker.com/5953047/how-to-crack-wep-and-wpa-wi-fi-passwords
2. http://mods-n-hacks.wonderhowto.com/how-to/crack-wi-fi-passwords-for-beginners-0139793/
3. http://www.hackwifinow.com/
4. http://arstechnica.com/security/2012/08/wireless-password-easily-cracked/
5. http://www.wifi-hacker.org/